

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

INFORMATION ASSOCIATED WITH GOOGLE ACCOUNT
justinbdurham@gmail.com THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE, LLC.

Case No. 4:23 MJ 8219 SRW

SIGNED AND SUBMITTED TO THE COURT
FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. Sections 1001, 1512, 1591, 2251,
and 2252A

False Statements, Obstruction, Sex Trafficking of Children, Production of Child
Pornography, and Possession and Receipt of Child Pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Derek G. Velazco
Applicant's signature

Derek G. Velazco, Special Agent, FBI

Printed name and title

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: August 23, 2023

Steve Welby
Judge's signature

City and state: St. Louis, MO

Stephen R. Welby, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)	
INFORMATION ASSOCIATED WITH)	No. 4:23 MJ 8219 SRW
GOOGLE ACCOUNT)	
justinbdurham@gmail.com THAT IS)	
STORED AT PREMISES CONTROLLED)	FILED UNDER SEAL
BY GOOGLE, LLC.)	

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Derek G. Velazco, a Special Agent with the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41 for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Google, LLC, (hereinafter “the Provider”), an email provider, headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. The search warrant would require the Provider to disclose to the United States copies of the information (including the content of communications) further described in Attachment B. Upon receipt of the information described in Section I of Attachment B, United States-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I, Derek G. Velazco, am a Special Agent with the Federal Bureau of Investigation (FBI) in the St. Louis Division. I have been an FBI agent since March 2017. Additionally, I have been employed with the FBI for a total of 16 years, having served in several administrative and

analytical roles prior to becoming a Special Agent. In the course of my duties, I have investigated both criminal and national security matters for my agency and in partnership with various other criminal investigative and intelligence agencies. These investigations have included terrorism and counterintelligence; however, the majority of my investigations have been related to violent crimes committed against children or human trafficking. I have received and provided training matters related to violent crimes against children and human trafficking.

3. The facts in this Affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This Affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1001 (false statements), 1512 (obstruction), 1591 (sex trafficking of children), 2251 (production of child pornography), and 2252A (possession and receipt of child pornography), have been committed by Justin Bradley Durham. There is also probable cause to search the location described in Attachment A for the information described in Attachment B for evidence of these crimes.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

LOCATION TO BE SEARCHED

6. The location to be searched is:

Google account **justinbdurham@gmail.com** (hereinafter referred to as “**subject account**”) located at Google, LLC., 1600 Amphitheatre Parkway, Mountain View, CA 94043, further described in Attachment A. The items to be reviewed and seized are described in Attachment B..

BACKGROUND CONCERNING EMAIL

7. In my training and experience, I have learned that the Provider provides a variety of on-line services, including electronic mail (“email”) access, to the public. The Provider allows subscribers to obtain email accounts at the domain name **gmail.com**., like the email account listed in Attachment A. Subscribers obtain an account by registering with the Provider. During the registration process, the Provider asks subscribers to provide basic personal information. Therefore, the computers of the Provider are likely to contain stored electronic communications (including retrieved and unretrieved email for the Provider subscribers) and information concerning subscribers and their use of the Provider services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

8. Subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by the Provider. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

9. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such

information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

10. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

11. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a

result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to

commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

13. In general, an email that is sent to the Provider is stored in the subscriber's "mail box" on the Provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the Provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the Provider's servers for an extended period of time and, in some circumstances, indefinitely.

BACKGROUND CONCERNING GOOGLE

14. I have learned the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under the domain name gmail.com. A subscriber using the Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents.* In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol (“IP”) address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber’s means and source of payment, including any credit card or bank account number.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Android ID, Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at Google using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways they do that is by using cookies, a string of characters stored on the user’s computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google also typically retains certain

transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google’s websites). Google also retains information regarding accounts registered from the same IP address.

vii. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber’s account.

viii. *Preserved and backup records.* Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

15. In addition, Google maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

a. *Google Drive content.* Google provides users with a certain amount of free “cloud” storage, currently 15 gigabytes, through a service called “Google Drive” (users can purchase a storage plan through Google to store additional content). Users can purchase enhanced storage capacity for an additional monthly fee. Users can use their Google Drive to store email, attachments, videos, photographs, documents, and other content “in the cloud,” that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google provides users with the ability to write, edit, and collaborate on various documents with other Google users through a service called “Google Docs.” Users can use Google Docs to create online documents that can be stored on or saved to the user’s Google Drive.

c. *Google Photos.* Google provides users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or “Exif”) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in “chat” sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in a user’s email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user’s email and chat content.

f. *Location History data.* Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or “apps”) or services provided by Google. For example, Google collects information collected from GPS, Wi-Fi networks, cell site locations, and mobile networks to estimate a user’s location. Google apps and services also allow for location reporting, which allows Google to periodically store and use a device’s most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Google Profile.* Google allows individuals to create a Google profile with certain identifying information, including pictures.

i. *Google Plus.* Google hosts an Internet-based social network. Among other things, users can post photos and status updates and group different types of relationships (rather than simply “friends”) into Circles. In addition, Google has a service called PlusOne, in which Google recommends links and posts that may be of interest to the account, based in part on accounts in the user’s Circle having previously clicked “+1” next to the post. PlusOne information therefore provides information about the user of a given account, based on activity by other individuals the user has entered in the user’s Circle.

j. *Chrome Browser and Search History.* Google stores information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at <http://www.google.com> (and variations thereof, including

<http://www.google.ru>), and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

k. *Advertising Data.* Google also stores advertising data, including information regarding unique advertising IDs associated with the customer, devices used to access the account, application IDs, advertising cookies, Unique Device Identifiers (UDIDs), payment information, ads clicked, and ads created.

l. *YouTube Data.* Google owns the video-streaming service YouTube and maintains records relating to YouTube accesses and data posted by the user.

16. Therefore, the computers of Google and are likely to contain stored electronic communications (including retrieved and unretrieved email) for Google subscribers and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. As explained above, Google subscribers can also store with the providers files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

18. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other

identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

19. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by

the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

21. Most individuals who collect child pornography are sexually attracted to children, as their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences involving children. Collectors of child pornography express their attraction to children through the collection of sexually explicit materials involving children, as well as other seemingly innocuous material related to children.

22. The above-described individuals may derive sexual gratification from actual physical contact with children, as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding

motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

23. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," further defined as any material relating to children that serves a sexual purpose for a given individual. "Child erotica" is broader and more encompassing than child pornography, though at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his/her intent. "Child Erotica" includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

24. Child pornography collectors often reinforce their fantasies by taking progressive, overt steps aimed at turning such fantasy(ies) into reality in some, or all, of the following ways: collecting and organizing their child-related material; masturbating while viewing child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children, thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to

which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

25. Child pornography collectors almost always maintain and possess their material(s) in the privacy and security of their homes or some other secure location, to include Internet cloud storage, such as Dropbox, Box, and Google cloud storage. The collection may include sexually explicit or suggestive materials involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is often aroused while viewing the collection and, acting on that arousal, he/she often masturbates, thereby fueling and reinforcing his/her attraction to children.

26. Due to the fact that the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document the seduction of children treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector deletes files from his hard drive or other electronic media, a computer expert is often able to retrieve those files using computer forensic tools.

PROBABLE CAUSE

27. On March 1, 2023, the St. Louis Division of the FBI opened an investigation into Justin Bradley Durham based on reporting provided by a sensitive financial source. Based on the source reporting, PayPal account associated with “Justin Durham” was used to conduct a purchase believed to be associated with child pornography.

28. The same reporting provided associated account information, to include phone number 573-647-1944 and email address justin_b_durham@yahoo.com. FBI analysts in the St. Louis Division conducted open-source records checks for the above email address and phone number. The results indicated the contact information to be associated with Justin Durham.

29. Your affiant also discovered that Durham is employed as a Deputy with the Phelps County Sheriff's Office. Durham began his employment with Phelps County as a certified deputy/corrections officer on August 12, 2013. He subsequently became a full-time deputy on May 23, 2014. As part of his assigned duties, Durham is assigned to work with the County's sex offenders. Additionally, Durham works with a youth program at the Sheriff's Office.

30. Additional open-source research conducted by FBI analytic personnel identified a Dropbox account believed to be associated with Durham and his communication account. Subsequently, administrative subpoenas were created for the subject account and served to Dropbox.

31. As part of the investigation, FBI analytics contacted PayPal and requested additional supporting documentation associated with Durham's account. PayPal provided records for several accounts, some of which did not have activity. However, for the specific account which was assessed to be involved in the purchase of child pornography (account# 1619260006658666785), the company provided a spreadsheet with purchase records. These records included several purchases from retailers such as Walmart, Wayfair, Etsy, Urban Outfitters, REVOLVE, Fanatics, and Papa Johns amongst others. Also included in these records are several purchases from individual names, to include "Maya Reyes," a name associated with the original reporting of child pornography purchases.

32. The aforementioned account, associated with the email address justin_b_durham@yahoo.com, was established on July 20, 2021. Records provided by PayPal indicate purchases made in the account occurred between July 20, 2021, and March 25, 2022. In the course of the investigation, FBI personnel observed five separate purchases with characteristics matching the original purchase of interest.¹

33. On June 2, 2023, your affiant, as well as FBI Special Agents Jason Hamlin and Tyler Roby, approached Durham at his residence, i.e. Premises #1. The investigators informed Durham about the ongoing investigation and asked about his involvement in the potential purchase of child pornography. Durham denied any involvement in the purchase of child pornography. Additionally, Durham denied having a PayPal account and stated he had an account “years ago” and that someone, whom Durham did not know, had committed fraud on his account. Durham made a report to the company about the fraud. When he attempted to establish an account at a later time, he was denied. In July 2023, FBI personnel contacted PayPal to inquire if the company was able to locate any complaints made by Durham. The company was unable to confirm any complaints had ever been made.

34. Durham stated he was not familiar with the name “Maya Reyes” and had never purchased child pornography using the Internet. Durham acknowledged the email address, phone number, and credit card number associated with the PayPal account were his. He also stated his home internet was password protected. When asked who else would have access to these accounts,

¹ These characteristics include purchases for small amounts of money, with round totals (e.g. \$40.00), paid to individuals, not specific companies, many of which were associated with female names.

Durham suggested only his daughter, C.D., would have the same access. At the time of the purchases of interest, C.D. would have been a minor.

35. Durham stated he previously had a Dropbox account, which he had not accessed for years. He stated this account was used to maintain images from his time in the Army.

36. Durham was asked to submit to a search of his phone and to complete a polygraph. Durham stated he would not consent to a search of his phone but would possibly be willing to take a polygraph. However, Durham stated he obtained a new phone “a couple of weeks ago.”

36. Durham was allowed to review the purchases from PayPal account# 1619260006658666785 which included a purchase from Maya Reyes, as well as other individuals. This account also had purchases such as jeans, a mirror, a St. Louis Blues jersey, pizza, and pajamas. Durham stated he did not make these purchases and insinuated it was likely C.D. who made the purchases. Durham also stated he would like to speak with C.D. prior to investigators approaching her. During a phone call on July 6, 2023, PayPal confirmed the same “VID” was used to access the account approximately 30 times between July 2021 and April 2022. The VID is also the same one which was used to access the account on January 27, 2022, the day during which the questionable purchases from the “Maya Reyes” account occurred.²

37. On June 16, 2023, SA Roby and SA Hamlin conducted an interview of C.D. at the Rolla Resident Agency of the FBI. During the interview, C.D. stated she did not have a PayPal account and never created an account under Durham’s name. Additionally, C.D. stated she has

² The “VID” is an internal PayPal terminology (number) used to describe a specific device, utilizing a specific browser to access an account. If a device were to use multiple browsers, multiple VIDs would be generated. At present, the FBI has not been able to match the aforementioned VID to a specific device in Durham’s possession.

never used Durham's credit card without his permission. C.D. stated that several of the items listed in the PayPal transaction records were purchases made for her by Durham, to include the St. Louis Blues jersey and a heart shaped mirror.

38. C.D. stated she would locate items she liked online and then inform Durham who would make the purchases. C.D. also stated she had never bought or sold illicit images via PayPal.

39. On June 16, 2023, SA Roby and SA Hamlin also spoke with Durham who had accompanied C.D. to the FBI office. Durham stated he was no longer willing to take a polygraph. Additionally, Durham stated he only had a cellular phone and did not possess a computer. Durham stated he would allow a limited search of his cellular phone, but after his initial interview with the FBI, Durham damaged his cellular phone while camping the same weekend and was forced to buy a new phone. Durham stated he went to the AT&T store to get the cellular phone fixed but was quoted a price which was too high and opted to purchase a new cellular phone instead. Durham stated he did not trade his old cellular phone in, but simply threw it out after purchasing his new cellular phone.

40. On June 16, 2023, SA Roby went to the AT&T store located at 119 South Bishop Ave., Rolla, MO. SA Roby conducted an interview with D.S., an employee of the store. D.S. stated Durham came into the store on June 4, 2023. At this time, Durham purchased a new cellular phone and had the data moved from his old cellular phone to his new one. The old cellular phone was then returned to Durham. D.S. also stated the old cellular phone was not observed to be damaged by AT&T staff and was still in working condition. AT&T staff did not provide a quote for fixing the "damaged" phone.

41. On June 28, 2023, in response to an Administrative Subpoena sent to Dropbox, the company provided records related to the account associated with "Jamea Dean" and email address

justin_b_durham@yahoo.com. These records indicated the account had been accessed numerous times. IP information from “authentication logs” was provided. These logs included IP information from November 21, 2022, through June 4, 2023.

42. The records also indicated the account had a fee of \$119.88 which was charged on July 20, 2021, and then again on July 20, 2022. The records also indicate the account has now been disabled. However, the “authentication logs” show activity on June 4, 2023.

43. FBI analysis of Dropbox records showed the Dropbox account assessed to be associated with Durham was accessed within an hour of the purchases made from the “Maya Reyes” account captured on PayPal records and reporting.

44. On July 12, 2023, United States Magistrate Judge Shirley Mensah signed a federal search warrant for the Dropbox account associated with email address justin_b_durham@yahoo.com.

45. On or about July 19, 2023, Dropbox responded to the search warrant by providing the contents of the aforementioned account. According to Dropbox, the account was active and logged into through mobile/authentication logs from November 16, 2017, through June 4, 2023 (which was two days after agents interviewed Durham at his residence and the last log in to the account). Information regarding the disabling of the account was requested from Dropbox. Dropbox reported they do not have this information to provide to investigators. The last IP activity in the account occurred on June 4, 2023.

46. The Dropbox production dated July 19, 2023, shows that there is no content in the account as of that same date. However, Dropbox did produce the contents of deleted files in the account, which is approximately 37 GB of data held in 23 different files folders, including ones named “mynudes”, “Selling”, “Trades”, “Alexs premium dropbox”, “girl on girl”, “Juicy fully

loaded !”, “136 photos and 13 videos copied on January 27, 2022”, and “working.” Dropbox has not disclosed when these files were deleted or the account was disabled.

47. Within the aforementioned folders in the deleted space, your affiant discovered hundreds of sexually explicit images and videos. Most of these images and videos appear to depict adult females; however, some images appear to be possible child pornography. For example, the following images appear to be child pornography:

a. “1631550381839742_Photo Sep 13, 10 00 26 AM.jpg” – a graphic image file that depicts an apparent nude minor female standing in front of a bathroom mirror holding a white cell phone; and

b. “1631550381839748_Photo Sep 13, 10 00 26 AM (9). jpg” – a graphic image file that depicts the same apparent minor female wearing a purple bra with her legs spread and her fingers touching her vagina.

Those images and others have been sent to the National Center for Missing and Exploited Children (NCMEC) for analysis. As of the date of this application, NCMEC has not yet responded.

48. The folder entitled “working” has approximately 35 different subfolders within it that have names such as “Ariel”, “Brenda”, “jess”, “b”, “random”, and “snapwhore”. Within these subfolders are images and videos of adult women engaged in sexually explicit activity. To date, the FBI has been able to identify the following:

a. In one of the subfolders are images and videos of the defendant exchanged in sexual intercourse with an adult female. Using facial recognition tools, the FBI was able to identify this female as V.S. On August 3, 2023, V.S. was interviewed by the FBI SA Velazco. V.S. stated that Durham is her cousin and that Durham had been sexually abusing her since she was approximately 9 or 11 years old (at the time, Durham was 14 years old). V.S. is now 37 years

old. V.S. believes that Durham sexually abused her when he was an adult and she was still a minor. Durham previously had threatened V.S. that if she did not continue having sex with him he would disclose their sexual relationship to others. V.S. believes that the images and videos found in the Dropbox account were taken at Durham's residence in Rolla, MO. V.S. last spoke to Durham about a week prior to the interview. In recent conversations he had asked for images of her breasts.

b. In another one of the subfolders are sexually explicit images of an adult female. Using facial recognition tools, the FBI was able to identify this female as A.A. On August 4, 2023, A.A. was interviewed by SA Roby. A.A. stated that Durham had previously forcibly raped her on several occasions, including at knife point. On one occasion, he handcuffed her to a bed and raped her. On another occasion, while in a police uniform, he traveled to her residence in Lake of the Ozarks, Missouri and sodomized her with an object. On a third occasion, Durham sexually assaulted A.A. resulting in significant damage to her genital region. As a result of this event, A.A. had to be hospitalized and received stitches to her vagina and anus. This last assault occurred while in Dent County, Missouri. During a fourth incident, Durham sexually assaulted A.A. while in a movie theatre in Rolla, Missouri. During this event, Durham allegedly forced A.A. to the ground and made her perform oral sex.

c. In another one of the subfolders are sexually explicit images of "Brenda." The FBI has identified Brenda as a part-time employee with Phelps County Sheriff's Office. Several of the images appear to depict Brenda engaged in sexual acts inside of the Phelps County Sheriff's Office facility.

d. In another one of the subfolders are three different videos of dogs performing oral sex on a female. To date, the FBI has not been able to identify the female(s) appearing in these videos.

49. Within the “working” folder is a subfolder entitled “text.” This subfolder contains screenshots of what appear to be sexually explicit text and social media communications between Durham and several others. To date, the FBI has been able to identify the following:

a. Your affiant has learned that one of the phone numbers is registered to K.B., who is a current assistant prosecuting attorney with Phelps County Prosecutors Office. There are more than 150 screenshots of messages with K.B. The filenames of these screenshots show dates occurring between June 2017 and November 2017. Your affiant notes that there is another subfolder under “working” that contains sexually explicit images and videos of K.B.

b. Your affiant has learned that another one of the phone numbers is associated with J.T. Your affiant notes that there is another subfolder under “working” that contains sexually explicit images of J.T. On July 31, 2023, J.T. was interviewed by the FBI SA Velazco. J.T. stated that she had a prostitution arrangement with Durham, whom she knew as “Jeff,” where Durham sent her money for sexually explicit images. In addition, Durham paid her for sex on approximately six different occasions.

c. Your affiant has learned that another one of the phone numbers is associated with T.F., who was an active sex worker in Missouri.

d. Your affiant has learned that another one of the phone numbers is associated with A.M. Your affiant notes that there is another subfolder under “working” that contains sexually explicit images of A.M. On August 2, 2023, SA Roby affiant interviewed A.M. A.M. stated that she met Durham through Facebook messenger in approximately 2017 and Durham

solicited her for sexual images. Durham asked A.M. to meet him for sex on several occasions but she never did. A.M. provided saved messages between her and Durham. In December of 2017, Durham told A.M. he could help her with a money issue but she would need to pay him back, but not with money. Durham then asked A.M. to “see something nude about you.” Durham asks A.M. about her experiences with sexual contact and dogs.

e. Your affiant has learned that another one of the phone numbers is associated with B.G. The screenshots for the text communications with B.G. are dated 2017. Your affiant has learned that B.G. was a minor female at that time. The screenshots show Durham and B.G. engaged in a discussion regarding the sexual activities of the minor. On July 27, 2023, B.G. was interviewed by the FBI SA Velazco. B.G. stated that Durham conducted a traffic stop of B.G. and her friends in 2017 and discovered marijuana in the vehicle. Subsequently, B.G. was called in to meet with the Phelps County prosecutor’s office and was told that Durham had put in a good word for B.G. Some time later, B.G. began receiving text messages from Durham, including ones where Durham told B.G. that she owed him one. Over the course of several years, Durham continued to attempt contact with B.G. This activity has continued through the last year.

50. On August 3, 2023, FBI agents again reviewed Dropbox IP addresses which revealed the Dropbox account associated with Durham was active and logged into from November 16, 2017, through June 4, 2023. The account was active and logged into through mobile/authentication logs until June 4, 2023; two days after your affiant interviewed Durham at his residence. The Dropbox account was disabled after June 4, 2023.

51. The June 4, 2023, log in was made by and through a T Mobile IP address. During the aforementioned interview with Durham, Durham stated that he uses T Mobile as his home

internet provider at his residence. In addition, during the aforementioned interview with C.D., C.D. stated that Durham uses a “puck” home internet device.

52. On August 8, 2023, United States Magistrate Judge Patricia Cohen signed federal search warrants for Durham’s residence and his Apple iPhone 14.

53. On August 9, 2023, Durham arrived at Phelps County Sheriff’s Office for work. At this time, his employment was terminated and was arrested and charged with possession of child pornography by the Phelps County Prosecuting Attorney. On the same day, the FBI executed the aforementioned search warrants at Durham’s residence and on his Apple iPhone 14 (which was in Durham’s possession).

54. Following Durham’s arrest, the Phelps County Sheriff’s Office issued a press release requesting anyone with negative encounters with Durham to contact the Missouri State Highway Patrol (MSHP). As of the date of this affidavit, at least 4 different individuals have come forward with information about Durham.

55. On August 15, 2023, the MSHP interviewed E. E. stated that she met Durham when she was 16 years old (she is now approximately 25 years old). E. was trying to find her real father and believed that Durham’s brother, Jeffrey, may have been her father. At the time, E. had a boyfriend, was homeless and was using marijuana and pills. E. contacted Durham because she needed money and he paid her and her boyfriend for sexually-explicit pictures on several occasions. E.’s boyfriend also found others who were willing to pay for sexually explicit pictures of E. E. stated that Durham knew that she was a minor and that he told her that he thought that was hot. On one occasion, E.’s boyfriend drove her to meet up with Durham in his police car in a secluded parking lot. E. remembers that Durham was wearing his uniform and he put his hand on her leg. On another occasion, E. told Durham she needed \$200 for a hotel and Durham responded

that she needed to earn that from him. E.'s boyfriend drove her to Durham's residence where Durham had vaginal intercourse with E. and he ejaculated on her face. Afterwards, Durham paid \$200 cash to E.

56. A forensic review of the Apple iPhone 14 shows several of the media files contained in the aforementioned "working" folder from Dropbox were also located on the device. Additionally, some of the images which were located on the phone were determined to be CSAM images of "E," a minor female victim. Other images depict V.S. (as an adult), the previously mentioned victim of a sexual assault by Durham.

57. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

58. For example, the stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

59. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-

location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

60. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

61. Other information connected to a Google account may lead to the discovery of additional evidence. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED


62. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require the Provider to disclose to the United States copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

63. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on the Provider. Because the warrant will be served on the Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

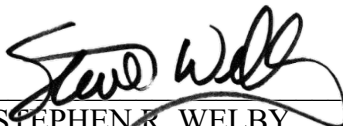
64. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

I state under the penalty of perjury that the foregoing is true and correct.



DEREK G. VELAZCO
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, or affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on August 23, 2023.



STEPHEN R. WELBY
United States Magistrate Court Judge
Eastern District of Missouri

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Google account, associated with email **justinbdurham@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google, LLC. (“Google”), which is headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. The content of all communications sent to or from the account (including through Gmail, Google Hangouts (including videos), and otherwise), stored in draft form in the account, or otherwise associated with the account, including all message content, attachments, and header information;
2. All address book, contact list, or similar information associated with the account;
3. Full Google search history and Chrome browser history associated with the account;
4. All Google Drive content;
5. All bookmarks maintained by the account;
6. All services used by the account;
7. All subscriber and payment information, including full name, e-mail address (including any secondary or recovery email addresses), physical address (including city, state, and

zip code), date of birth, gender, hometown, occupation, telephone number, websites, screen names, user identification numbers, security questions and answers, registration IP address, payment history, and other personal identifiers;

8. All past and current usernames, account passwords, and names associated with the account;

9. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;

10. All YouTube data associated with the account;

11. All transactional records associated with the account, including any IP logs or other records of session times and durations;

12. Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”), and any other information regarding the types of devices used to access the account;

13. All activity logs for the account;

14. All photos and videos uploaded to the account, including in Google Drive and Google Photos;

15. All information associated with Google Plus, including the names of all Circles and the accounts grouped into them;

16. All photos and videos uploaded by any user that have that user tagged in them;
17. All location and maps information;
18. All Google Voice information;
19. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
20. All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;
21. Advertising and Device Data: All advertising data relating to the account, including, but not limited to, advertising cookies, information regarding unique advertising IDs associated with the user, any devices used to access the account, Android IDs, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), ads clicked, and ads created;
22. Linked Accounts: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);
23. For accounts linked by cookie, the date(s) on which they shared a cookie;
24. For accounts linked by SMS number, information regarding whether the numbers were verified; and
25. Customer Correspondence: All records pertaining to communications between the Service Provider and any person regarding the user or the user's account with the Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber; and

26. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 DAYS** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1001 (false statements), 1512 (obstruction), 1591 (sex trafficking of children), 2251 (production of child pornography), and 2252A (possession and receipt of child pornography) involving Justin Bradley Durham from 2014 to Present, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Any evidence showing that Durham made false statements to federal agents, including but not limited to his use of and access to PayPal, Dropbox or other file sharing programs;
- (b) Any evidence related to the use of PayPal to make purchases between July 2021 and March 2022;
- (c) Any evidence related to the use of Dropbox;
- (d) Any evidence showing that Durham destroyed or disabled evidence, including but not limited to his Dropbox account, his cellular phone, and/or his Apple iCloud account;

- (e) All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
- (f) Any and all documents, records, materials, emails, and/or internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to an interest in child pornography whether transmitted or received.
- (g) Any evidence related to the sex trafficking of minors;
- (h) Any communications with C.D., V.S., K.B., B.G., or E.;
- (i) The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- (j) Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- (k) Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- (l) Evidence indicating the subscriber's state of mind as it relates to the crimes under investigation; and
- (m) Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.
- (n) information indicating how and when the email account was accessed or used, to

- determine the geographic and chronological context of account access, use, and events relating to the crime(s) under investigation and to the email account owner;
- (o) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any United States personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, analysts, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the United States and their support staff for their independent review.